????

Harley Eades III

Computer Science
Augusta University
harley.eades@gmail.com

Abstract. TODO

1 Introduction

2 A Quaternary Semantics for SAND Attack Trees

Kordy et al. [1] gave a very elegant and simple semantics of attack-defense trees in boolean algebras. Unfortunately, while their semantics is elegant it does not capture the resource aspect of attack trees, it allows contraction, and it does not provide a means to model sequential conjunction. In this section we give a semantics of attack trees in the spirit of Kordy et al.'s using a four valued logic.

The propositional variables of our ternary logic, denoted by A, B, C, and D, range over the set $\mathsf{Four} = \{0, \frac{1}{4}, \frac{1}{2}, 1\}$. We think of 0 and 1 as we usually do in boolean algebras, but we think of $\frac{1}{4}$ and $\frac{1}{2}$ as intermediate values that can be used to break various structural rules. In particular we will use these values to prevent exchange for sequential conjunction from holding, and contraction from holding for parallel and sequential conjunction.

Definition 1. *The logical connectives of our four valued logic are defined as follows:*

Parallel Conjunction:

$$\begin{array}{l} A \odot_4 B = 1, \textit{where neither } A \textit{ nor } B \textit{ are } 0 \\ A \odot_4 B = 0, \textit{otherwise} \end{array}$$

Sequential Conjunction:

$$\begin{array}{l} \frac{1}{4} \rhd_4 B = \frac{1}{4}, \textit{where } B \neq 0 \\ A \rhd_4 B = \frac{1}{2}, \textit{where } A \in \{\frac{1}{2}, 1\} \textit{ and } B \neq 0 \\ A \rhd_4 B = 0, \textit{otherwise} \end{array}$$

Choice: $A \sqcup_4 B = \mathsf{max}(A, B)$

These definitions are carefully crafted to satisfy the necessary properties to model attack trees. Comparing these definitions with Kordy et al.'s [1] work we can see that choice is defined similarly, but parallel conjunction is not a product – ordinary conjunction – but rather a linear tensor product, and sequential conjunction is not actually definable in a boolean algebra, and hence, makes heavy use of the intermediate values to insure that neither exchange nor contraction hold. The following results solidify these claims.

We use the usual notion of equivalence between propositions, that is, propositions ϕ and ψ are considered equivalent, denoted by $\phi \equiv \psi$, if and only if they have the same truth tables. In order to model attack trees parallel conjunction must be symmetric, associative, but not satisfy contraction.

Lemma 1 (Parallel Conjunction is Symmetric). *For any A and B, $A \odot_4 B \equiv B \odot A$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 2 (Parallel Conjunction is Associative). *For any A, B, and C, $(A \odot_4 B) \odot_4 C \equiv A \odot_4 (B \odot_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 3 (Parallel Conjunction is not Contractive). *It is not the case that for any A, $A \odot_4 A \equiv A$.*

Proof. Suppose $A = \frac{1}{4}$. Then by definition $A \odot_4 A = 1$, but $\frac{1}{4}$ is not 1.

Similarly, sequential conjunction must be associative, but not symmetric nor satisfy contraction.

Lemma 4 (Sequential Conjunction is Associative). *For any A, B, and C, $(A \rhd_4 B) \rhd_4 C \equiv A \rhd_4 (B \rhd_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 5 (Sequential Conjunction is not Symmetric). *It is not the case that for any A and B, $A \rhd_4 B \equiv B \rhd_4 A$.*

Proof. Suppose $A = \frac{1}{4}$ and $B = \frac{1}{2}$. Then $A \rhd_4 B = \frac{1}{4}$, but $B \rhd_4 A = \frac{1}{2}$.

Lemma 6 (Sequential Conjunction is not Contractive). *It is not the case that for any A, $A \rhd_4 A \equiv A$.*

Proof. Suppose $A = 1$. Then by definition $A \odot A = \frac{1}{2}$, but $\frac{1}{2}$ is not 1.

Now choice satisfies all three properties, that is, it is symmetric, associative, and does satisfy contraction.

Lemma 7 (Choice is Symmetric). *For any A and B, $A \sqcup_4 B \equiv B \sqcup_4 A$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 8 (Choice is Associative). *For any A, B, and C, $(A \sqcup_4 B) \sqcup_4 C \equiv A \sqcup_4 (B \sqcup_4 C)$.*

Proof. This proof holds by simply comparing truth tables.

Lemma 9 (Choice is Contractive). *For any A, $A \sqcup_4 A \equiv_4 A$.*

Proof. This proof holds by simply comparing truth tables.

Finally, the necessary distributive laws hold.

Lemma 10 (Parallel Conjunction Distributes Over Choice).

i. For any A, B, and C, $A \odot_4 (B \sqcup_4 C) \equiv (A \odot_4 B) \sqcup_4 (A \odot_4 C)$.
ii. For any A, B, and C, $(A \sqcup_4 B) \odot_4 C \equiv (A \odot_4 C) \sqcup_4 (B \odot_4 C)$.

Proof. This proof holds by simply comparing truth tables.

Lemma 11 (Sequential Conjunction Distributes Over Choice).

i. For any A, B, and C, $A \rhd_4 (B \sqcup_4 C) \equiv (A \rhd_4 B) \sqcup_4 (A \rhd_4 C)$.
ii. For any A, B, and C, $(A \sqcup_4 B) \rhd_4 C \equiv (A \rhd_4 C) \sqcup_4 (B \rhd_4 C)$.

Proof. This proof holds by simply comparing truth tables.

At this point it is quite easy to model attack trees as formulas. The following defines their interpretation.

Definition 2. *Suppose $\mathbb{B}$ is some set of base attacks, and $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then we define the interpretation of ATerms to propositions as follows:*

$$\begin{array}{ll}
[\![\mathbf{b} \in \mathbb{B}]\!] & = \alpha(\mathbf{b}) \\
[\![\mathsf{AND}\ T_1\ T_2]\!] & = [\![T_1]\!] \odot [\![T_2]\!] \\
[\![\mathsf{SAND}\ T_1\ T_2]\!] & = [\![T_1]\!] \rhd [\![T_2]\!] \\
[\![\mathsf{OR}\ T_1\ T_2]\!] & = [\![T_1]\!] \sqcup [\![T_2]\!]
\end{array}$$

We can use this semantics to prove equivalences between attack trees.

Lemma 12 (Equivalence of Attack Trees in the Ternary Semantics). *Suppose $\mathbb{B}$ is some set of base attacks, and $\alpha : \mathbb{B} \longrightarrow \mathsf{PVar}$ is an assignment of base attacks to propositional variables. Then for any attack trees T_1 and T_2, $T_1 \approx T_2$ if and only if $[\![T_1]\!] \equiv [\![T_2]\!]$.*

Proof. This proof holds by induction on the form of $T_1 \approx T_2$.

This is a very simple and elegant semantics, but it also leads to a more substantial theory.

3 Lineale Semantics for SAND Attack Trees

Classical natural deduction has a semantics in boolean algebras, and so the semantics in the previous section begs the question of whether there is a natural deduction system that can be used to reason about attack trees. We answer this question in the positive, but before defining the logic we first build up a non-trivial concrete categorical model of our desired logic in dialectica spaces, but this first requires the refinement of the quaternary semantics into a postal semantics we call the lineale semantics of SAND attack trees. This semantics will live at the base of the dialectica space model given in the next section.

We denote by $\leq_4\colon \mathsf{Four} \times \mathsf{Four} \to \mathsf{Four}$ the obvious preorder on Four making $(\mathsf{Four}, \leq_4)$ a preordered set. It is well known that every preordered set induces a category whose objects are the elements of the carrier set, here Four, and morphisms $\mathsf{Hom}_{\mathsf{Four}}(a, b) = a \leq_4 b$. Composition of morphisms hold by transitivity and identities exists by reflexivity. Under this setting it is straightforward to show that for any propositions ϕ and ψ over Four we have $\phi \equiv \psi$ if and only if $\phi \leq_4 \psi$ and $\psi \leq_4 \psi$. Thus, every result proven for the logical connectives on Four in the previous section induce properties on morphisms in this setting.

In addition to the induced properties just mentioned we also have the following new ones which are required when lifting this semantics to dialectica spaces, but are also important when building a corresponding logic.

Lemma 13 (Parallel Conjunction is Functorial). *For any $a, b, c, d \in \mathsf{Four}$, if $a \leq_4 c$ and $b \leq_4 d$, then $(a \odot_4 b) \leq_4 (c \odot_4 d)$.*

Proof. This proof holds by a straightforward case analysis on a, b, c, and d. In any cases where $(a \odot_4 b) \leq_4 (c \odot_4 d)$ does not hold, then one of the premises will also not hold.

Lemma 14 (Sequential Conjunction is Functorial). *For any $a, b, c, d \in \mathsf{Four}$, if $a \leq_4 c$ and $b \leq_4 d$, then $(a \rhd_4 b) \leq_4 (c \rhd_4 d)$.*

Proof. This proof is similar to the previous result.

Lemma 15 (Choice is Functorial). *For any $a, b, c, d \in \mathsf{Four}$, if $a \leq_4 c$ and $b \leq_4 d$, then $(a \sqcup_4 b) \leq_4 (c \sqcup_4 d)$.*

Proof. This proof is similar to the previous result.

The logic we a building up is indeed intuitionistic, but none of the operators we have introduced thus far are closed, but we can define the standard symmetric linear tensor product in Four that is closed.

Definition 3. *The following defines the linear tensor product on Four as well as linear implication:*

Tensor Product:

$$\begin{array}{l} A \otimes_4 B = \mathsf{max}(A, B), \textit{where } A \textit{ nor } B \textit{ are } 0 \\ A \otimes_4 B = 0, \textit{otherwise} \end{array}$$

The unit of the tensor product is $I_4 = \frac{1}{4}$.

Linear Implication:

$$\begin{array}{l} A \multimap_4 B = 0, \textit{where } B <_4 A \\ A \multimap_4 A = A, \textit{where } A \in \{\frac{1}{4}, \frac{1}{2}\} \\ A \multimap_4 B = 1, \textit{otherwise} \end{array}$$

The expected monoidal properties hold for the tensor product.

Lemma 16 (Tensor is Symmetric Monoidal).

(Symmetry) For any A *and* B*,* $A \otimes_4 B \equiv B \otimes A$*.*
(Associativity) For any A*,* B*, and* C*,* $(A \otimes_4 B) \otimes_4 C \equiv A \otimes_4 (B \otimes_4 C)$*.*
(Left Unitor) For any A*,* $(A \otimes I_4) \equiv A$*.*
(Right Unitor) For any A*,* $(I_4 \otimes A) \equiv A$*.*
(Functorality) For any A*,* B*,* C*, and* D*, if* $A \leq_4 C$ *and* $B \leq_4 D$*, then* $(A \otimes_4 B) \leq_4 (C \otimes_4 D)$*.*

References

1. Barbara Kordy, Marc Pouly, and Patrick Schweitzer. Computational aspects of attack–defense trees. In Pascal Bouvry, MieczysławA. Kłopotek, Franck Leprévost, Małgorzata Marciniak, Agnieszka Mykowiecka, and Henryk Rybiński, editors, *Security and Intelligent Information Systems*, volume 7053 of *Lecture Notes in Computer Science*, pages 103–116. Springer Berlin Heidelberg, 2012.

Appendix